

09/938, 790

(SH)

Amendments to the Specification:

Please replace the paragraph on page 14, line 10, which starts with "Note that".

Note that random material ~~materials~~, be it Pads or Keys, ultimately comes from the Server. In one embodiment, the Server is absolutely physically secured, with a very high quality, fast PRNG inside it that is fed bits by a high quality RNG.

Please replace the paragraph on page 17, line ⁹~~22~~, which starts with "

Referring to Figure 15, for encryption the Cipher machinery (1526) takes as input two Working Pads, derived from the four Source Pads (1506, 1508, 1510, 1512), two Working Keys (1532), two Rotation Values (1534), and the Clear Text data (1528). The two Working Pads each comes from one of the two Nested Shuffle & Substitution Machineries (1502, 1504). One machinery (1502) takes as input two Source Pads A and B (1506, 1508), two Substitution Keys A and B (1514), and two sets of three Mixing Keys (1516, 1518). The other machinery (1504) takes as input two Source Pads C and D (1510, 1512), two Substitution Keys C and D (1520), and, two sets of three Mixing Keys (1522, 1524) (~~1522, 1524~~). The Clear Text data (1528) cannot exceed half the length of a Source Pad, before requiring a new set of Working Keys and Rotation Values. For example, using four 16 MB Source Pads, a maximum of 8 MB of data can be encrypted before requiring a fresh set of two Working Keys and two Rotation Values. So every 8 MB block of encrypted data has a pair of Working Keys and a pair of Rotation Values associated with it. Every byte of Clear Text data is transformed out into a corresponding byte of Cipher Text data (1530), in a manner very similar to standard stream cipher behavior. The 1st clear byte becomes the 1st cipher byte, and the 2nd clear byte becomes the 2nd cipher byte, and so forth, until the last clear byte becomes the last cipher byte. However,